Cyber Security & Ethical Hacking Progetto

Malware Analysis

Per affrontare il progetto di analisi del malware, dobbiamo dividere il lavoro in due parti principali: l'analisi statica e l'analisi dinamica. Ecco una guida dettagliata per rispondere ai quesiti proposti:

Analisi Statica

1. **Parametri passati alla funzione Main**: 17

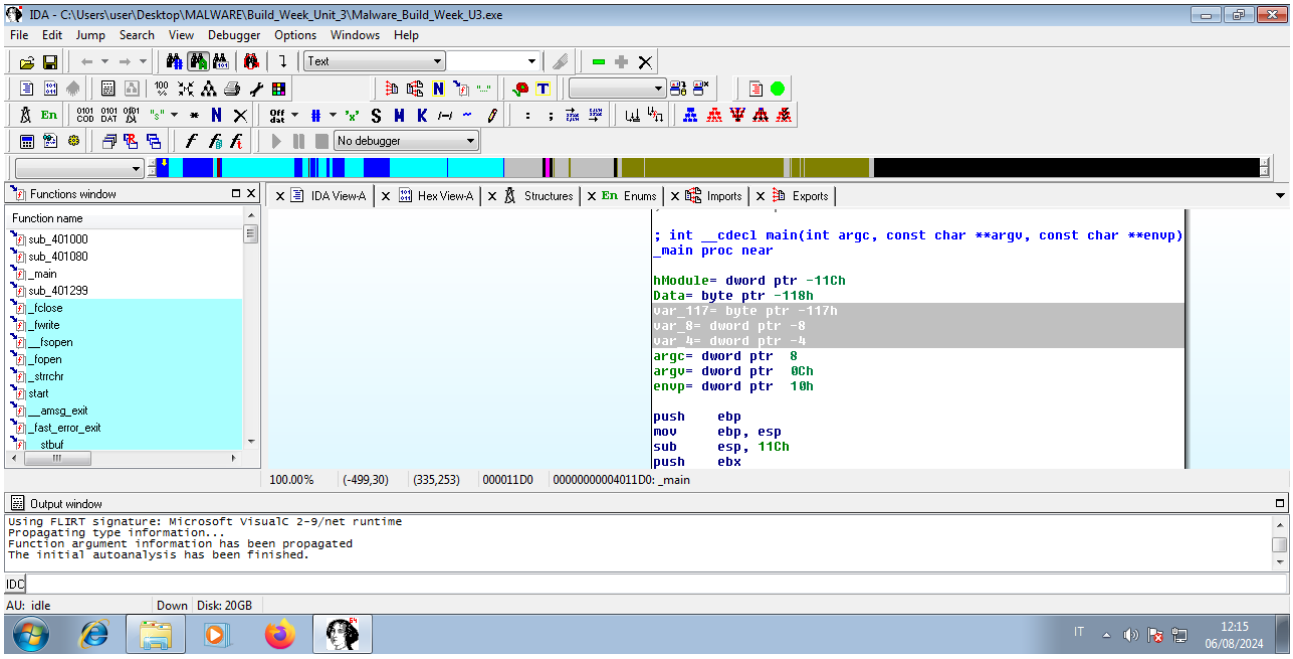
```
hModule= dword ptr -11Ch
Data= byte ptr -118h
var_117= byte ptr -117h
argc= dword ptr  8
envp= dword ptr  10h
push    ebp
mov     ebp, esp
sub     esp, 11Ch
call    ds:GetModuleHandleA
xor     eax, eax
lea     edi, [ebp+var_117]
rep stosd
stosb
add     esp, 4
or      ecx, 0FFFFFFFFh
pop     edi
retn
```

2. **Variabili dichiarate all'interno della funzione Main**: 3

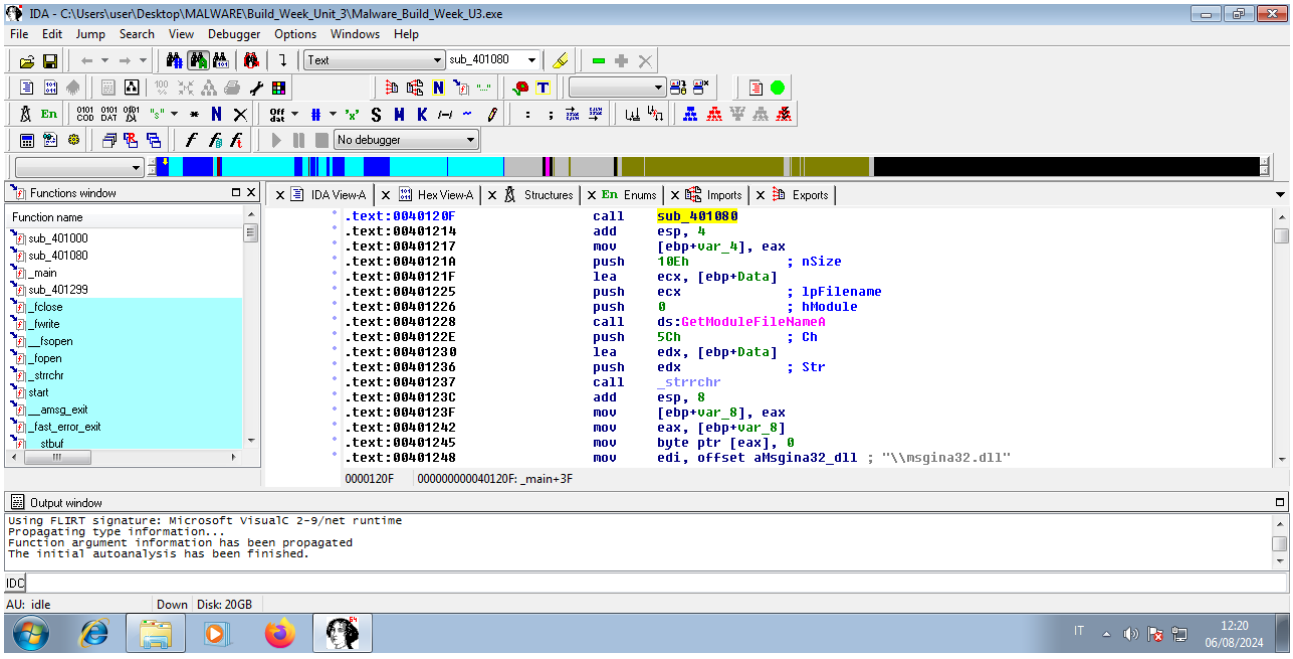
   var_117= byte ptr -117h

   var_8= dword ptr -8

   var_4= dword ptr -4

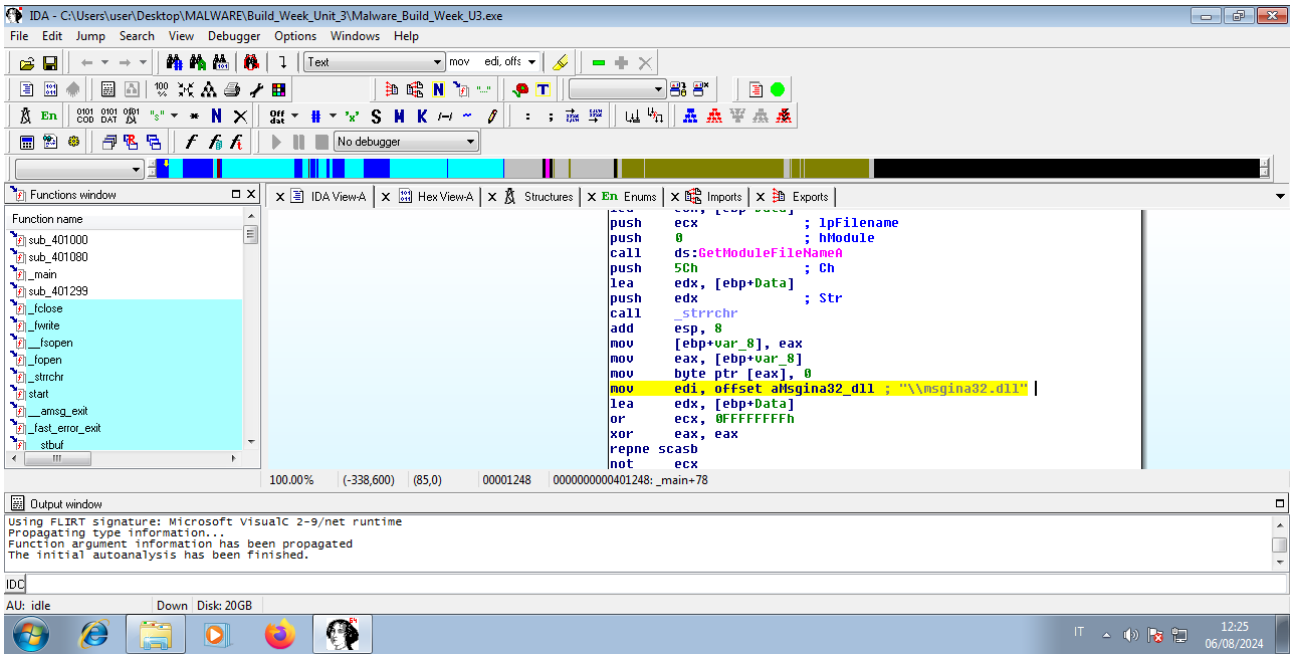


3. **Sezioni presenti all'interno del file eseguibile**:



4. **Librerie importate dal Malware**:

mov edi, offset aMsgina32_dll ; \\msgina32.dll



- **Lo scopo della funzione chiamata alla locazione di memoria 00401021:**
- .text:00401021 call ds:RegCreateKeyExA

- **Che oggetto rappresenta il parametro alla locazione 00401017:**
- push offset SubKey ; "SOFTWARE\\Microsoft\\Windows NT\\CurrentVe"...

- **Il significato delle istruzioni comprese tra gli indirizzi 00401027 e 00401029:**
- .text:00401027 test eax, eax
- .text:00401029 jz short loc_401032

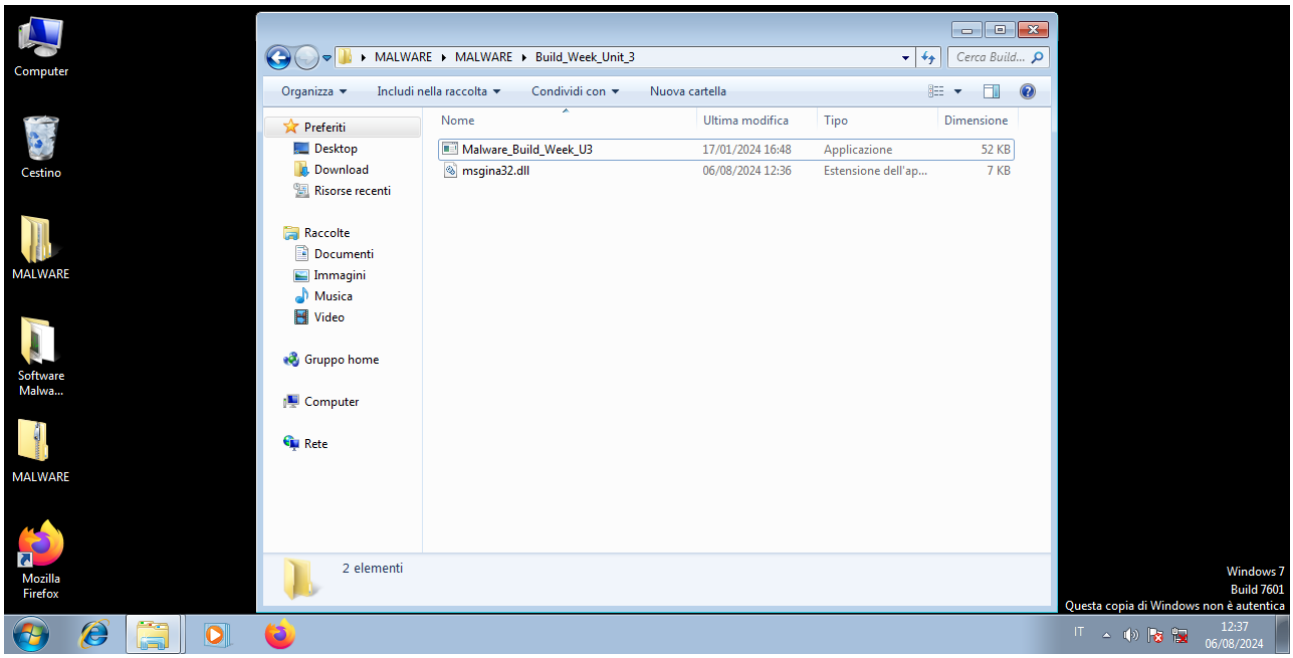
  Valutate ora la chiamata alla locazione 00401047, qual è il valore del parametro «ValueName»?

  call ds:RegSetValueExA

Analisi Dinamica

Cosa succede nella cartella dell'eseguibile del Malware?:

COMPORTMANETO MALEVOLE SULLA LIBRERIA MSGINA32.DLL



Analisi dei risultati di Process Monitor:

1. 11/20/2010 19:47:7 - PFRO Error:
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\New\mxdwdrv.dll,
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\mxdwdrv.dll, 0xc000003a
2. 11/20/2010 19:47:7 - PFRO Error:
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\New\unidrvui.dll,
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\unidrvui.dll, 0xc000003a
3. 11/20/2010 19:47:7 - PFRO Error:
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\New\UNIDRV.DLL,
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\UNIDRV.DLL, 0xc000003a
4. 11/20/2010 19:47:7 - PFRO Error:
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\New\UNIRES.DLL,
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\UNIRES.DLL, 0xc000003a
5. 11/20/2010 19:47:7 - PFRO Error:
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\New\XPSSVCS.DLL,
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\XPSSVCS.DLL, 0xc000003a
6. 11/20/2010 19:47:7 - PFRO Error:
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\New\mxdwdui.dll,
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\mxdwdui.dll, 0xc000003a
7. 11/20/2010 19:47:7 - PFRO Error:
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\New\FXSDRV.DLL,
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\FXSDRV.DLL, 0xc000003a
8. 11/20/2010 19:47:7 - PFRO Error:
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\New\FXSUI.DLL,
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\FXSUI.DLL, 0xc000003a

9. 11/20/2010 19:47:7 - PFRO Error:
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\New\FXSUI.DLL,
   \??\D:\Windows\system32\spool\DRIVERS\x64\3\FXSUI.DLL, 0xc000003a
10. 11/20/2010 19:47:7 - PFRO Error:
    \??\D:\Windows\system32\spool\DRIVERS\x64\3\New\FXSWZRD.DLL,
    \??\D:\Windows\system32\spool\DRIVERS\x64\3\FXSWZRD.DLL, 0xc000003a
11. 11/20/2010 19:47:7 - PFRO Error:
    \??\D:\Windows\system32\spool\DRIVERS\x64\3\New\FXSTIFF.DLL,
    \??\D:\Windows\system32\spool\DRIVERS\x64\3\FXSTIFF.DLL, 0xc000003a
12. 11/20/2010 19:47:7 - PFRO Error:
    \??\D:\Windows\system32\spool\DRIVERS\x64\3\New\FXSRES.DLL,
    \??\D:\Windows\system32\spool\DRIVERS\x64\3\FXSRES.DLL, 0xc000003a
13. 11/20/2010 19:47:7 - PFRO Error:
    \??\D:\Windows\system32\spool\DRIVERS\x64\3\New\FXSAPI.DLL,
    \??\D:\Windows\system32\spool\DRIVERS\x64\3\FXSAPI.DLL, 0xc000003a
14. 11/20/2010 19:47:7 - PFRO Error:
    \??\D:\Windows\system32\spool\drivers\x64\3\Old\1\FXSWZRD.DLL, |delete operation|,